CLAIMS

What is claimed is:

1. A method of controlling access to user-specific information for use in connection with a network computing environment including a web-services provider providing a web-based software service, a user of a service provided by the web-services provider, and a client of the web-services provider, said web-services provider maintaining a data store of user-specific information associated with the user in connection with the service, and said client seeking access to some of the user-specific information maintained in the data store, said method of controlling access to the user-specific information comprising:

obtaining an access request message from the client and directed to the software service requesting user-specific information, said request message including an access request parameter indicating the client's requested form of access to the user-specific information in the data store;

comparing the access request parameter to an access control list associated with the software service, said access control list identifying whether the user has granted the form of access requested by the client;

permitting the client to have access to the requested user-specific information in the data store if the user has granted the form of access requested by the client; and

invoking an access control engine if the user has not previously granted the form of access requested by the client, said access control engine:

determining an intended use by the client of the requested user-specific information in the data store;

comparing the determined intended use by the client with a default access control instruction;

updating the access control list to permit the client to have access to the requested user-specific information in the data store if the default access control instruction permits the determined intended use; and

transmitting a fault response to the client if the default access control instruction does not permit the determined intended use.

2. The method of claim 1 wherein comparing the determined intended use by the client with the default access control instruction further comprises comparing the client's requested form of access to the default access control instruction to determine if the default access control instruction permits the requested form of access.

3. The method of claim 1 wherein the client's requested form of access to the user-specific information in the data store identifies a desired subject matter to be accessed and a method of accessing the desired subject matter and wherein comparing the determined intended use by the client with the default access control instruction further comprises:

determining if the default access control instruction permits the client to access the desired subject matter; and

determining if the default access control instruction permits the identified method of accessing the desired subject matter.

4. The method of claim 1 wherein the user communicates with the web-services provider via a network communication device having a display interface and a selection interface, the method further comprising:

generating an option list having at least one entry therein based on the determined intended use by the client of the requested user-specific information in the data store;

displaying to the user on the display interface of the network communication device an option menu reflecting the generated option list, said option menu prompting the user to accept or reject at least one option using the selection interface of the network communication device;

receiving from the network communication device a selection signal indicative of whether the user accepted or rejected the at least one option; and

creating an access control rule based on the received selection signal, said access control rule defining the extent of access to the requested user-specific information in the data store granted to the client.

5. The method of claim 4 wherein creating the access control rule comprises updating the access control list such that the access control list reflects whether the user accepted or rejected the at least one option.

6. The method of claim 1 further comprising:

determining if the client has a local copy of the requested user-specific information in the data store before transmitting the access request message; and

retrieving said local copy of the requested user-specific information if the local copy is available;

determining if said local copy of the requested user-specific information is current; and

transmitting the access request message only if said local copy of the requested user-specific information is not available and not current.

7. The method of claim 1 further comprising authenticating a digital identity of the user and denying access to the requested user-specific information in the data store if the digital identity of the user is not authenticated.

8. The method of claim 1 wherein determining the intended use by the client of the requested user-specific information further comprises obtaining a copy of an intentions document associated with the client, said intentions document including a field being indicative of the intended use by the client of the requested user-specific information.

9. The method of claim 1 further comprising:

determining if the client has an access subscription right to the requested user-specific information in the data store; and

permitting the client to have access to the requested user-specific information in the data store if the client has the access subscription right to the requested user-specific information in the data store.

10. The method of claim 1 wherein permitting the client to have access to the requested user-specific information in the data store if the user has granted the form of access requested by the client further comprises:

permitting the client to read the requested user-specific information in the data store; and

permitting the client to write the requested user-specific information in the data store.

11. The method of claim 10 wherein permitting the client to read the requested user-specific information in the data store comprises accessing said requested user-specific information and transmitting a copy of the accessed requested user-specific information to the client in a SOAP message.

12. The method of claim 10 wherein permitting the client to write the requested user-specific information in the data store comprises receiving at the web-services provider a SOAP message from the client identifying the requested user-specific information and writing the identified requested user-specific information in the data store.

13. The method of claim 1 wherein updating the access control list to permit the client to have access to the requested user-specific information in the data store if the default access control instruction permits the determined intended use further comprises:

updating the access control list to permit the client to read the requested user-specific information in the data store; and

updating the access control list to permit the client to write the requested user-specific information in the data store.

14. One or more computer-readable media having computer-executable instructions for performing the method recited in claim 1.

15. A method of controlling access to user specific information for use in a network computer system including a web-services provider, a user of a service provided by the web-services provider, and a client of the web-services provider, said web-services provider maintaining a data store of user-specific information associated with the user and said client seeking access to the user-specific information in the data store, said method of controlling access to the user-specific information comprising:

operatively receiving at the web-services provider a request from the client to access the user-specific information in the data store;

determining an intended use by the client of the user-specific information in the data store;

determining an allowed level of access permitted by the user;

comparing the determined intended use with the determined allowed level of access; and

completing the request from the client to access the user-specific information in the data store when the determined intended use is within the determined allowed level of access.

16. The method of claim 15 wherein determining the intended use by the client of the user-specific information in the data store comprises:

determining a type of information within the user-specific information in the data store that is being requested by the client; and

determining a form of access to the user-specific information in the data store that is being requested by the client.

17. The method of claim 16 wherein comparing the determined intended use with the determined allowed level of access comprises:

determining if the user permits access to the type of information within the user-specific information in the data store that is being requested by the client; and

determining if the user permits the form of access to the user-specific information in the data store that is being requested by the client.

18. The method of claim 17 further comprising:

creating an access filter, said access filter defining an extent to which the user permits access to the type of information within the user-specific information in the data store and an extent to which the user permits the form of access to the user-specific information in the data store; and

wherein completing the request from the client to access the user-specific information in the data store when the determined intended use is within the determined allowed level of access further comprises:

applying the access filter to the user-specific information in the data store to create a filtered information set; and

permitting the client to access the filtered information set.

19. The method of claim 15 further comprising denying the client access to the requested user-specific information in the data store if the determined intended use is outside the allowed level of access.

20. The method of claim 15 further comprising invoking a consent engine if the determined intended use is outside the allowed level of access, said consent engine informing the user of the client's request to access the user-specific information in the data store and inviting the user to permit or to deny the client's request to access the user-specific information in the data store.

21. One or more computer-readable media having computer-executable instructions for performing the method recited in claim 15.

22. A user-centric method of controlling access to user specific information in a network computing environment, said network computing environment including a web-services provider and a user of a service provided by the web-services provider, the web-services provider maintaining a data store of use-specific information associated with the user, and the user communicating with the web-services provider via a network

communication device having a display interface and a selection interface, said user-centric method of controlling access to user-specific information comprising:

identifying the user;

identifying a client of the web-services provider to which the user desires to grant access to the user-specific information in the data store;

identifying a method of access by which the user is willing to allow the client to access the user-specific information in the data store;

identifying a level of access to the user-specific information in the data store the user desires to impose on the client; and

writing an access control rule to an access control list associated with said data store, said access control rule limiting access to the user-specific information in the data store by the client to the identified method and the identified level.

23. The method of claim 22 further comprising identifying a subscription status, said subscription status indicating whether the user intends the client to be notified if the user-specific information in the data store changes.

24. The method of claim 24 further comprising;

exposing a menu to the user on the display interface of the network communication device, said menu allowing the user to identify the client, the method of access, and the level of access; and

transmitting the identified client, the method of access, and the level of access to the web-services provider in a digital message format.

25. The method of claim 22 wherein identifying the method of access further comprises identifying whether the client is permitted to modify the user-specific information in the data store.

26. The method of claim 22 wherein identifying the level of access further comprises grouping the user-specific information in the data store into a plurality of

information types and identifying which of said plurality of information types the client may access.

27. The method of claim 22 further comprising:

authenticating a digital identity of the user prior to writing the access control rule to the access control list associated with the data store of user-specific information; and

writing the access control rule to said access control list only if the digital identity of the user is authenticated.

28. One or more computer-readable media having computer-executable instructions for performing the method recited in claim 22.

29. A system for controlling access to user-specific information in a network computing environment, the system comprising:

a web-services service provider;

a user of a service of the web-services provider, the web-services provider maintaining a data store of user-specific information associated with the user and a set of default access preferences defining a list of default access permissions allowed by the user;

a client of the web-services provider, said client requesting access to the data store of user-specific information associated with the user and identifying an intended use by the client of the user-specific information in the data store; and

an access control engine operatively receiving the client request to access the data store of user-specific information and dynamically creating an access control rule by comparing the set of default access preferences with the intended use by the client, said access control rule granting the requested access if the intended use of the client is within the list of default access permissions defined by the set of default access preferences.

30. The system of claim 29 further comprising a network communication device having a display interface and a selection menu and wherein the user communicates with the web-services provider via the network communication device.

31. The system of claim 30 further comprising a consent engine generating an option list having at least one entry therein based on the intended use by the client of the user-specific information in the data store, said consent engine displaying on the display interface of the network communication device an option menu reflecting the generated option list, said option menu prompting the user to accept or reject at least one option displayed on the option menu using the selection interface of the network communication device.

32. The system of claim 31 wherein the network communication device generates a selection signal indicative of whether the user accepted or rejected the at least one option displayed on the option menu.

33. The system of claim 31 wherein the consent engine provides a consent signal having a parameter indicative of whether the user accepted or rejected the at least one option and wherein the access control engine receives the consent signal, said access control engine granting the requested access if the consent signal indicates that the user accepted the at least one option.

34. The system of claim 33 wherein the access control engine denies the requested access if the consent signal indicates that the user rejected the at least one option.

35. The system of claim 29 further comprising an authentication engine authenticating a digital identity of the user and wherein the access control engine denies the requested access if the digital identity of the user is not authenticated by the authentication engine.

36. The system of claim 29 further comprising a client intentions document identifying the intended use by the client of the user-specific information in the data store.

37. The system of claim 36 further comprising:

a network communication device having a display interface and a selection menu and wherein the user communicates with the web-services provider via the network communication device; and

a consent engine retrieving the client intentions document and generating an option list having at least one entry therein based on the intended use identified in the intentions document, said consent engine displaying on the display interface of the network communication device an option menu reflecting the generated option list, said option menu prompting the user to accept or reject at least one option displayed on the option menu using the selection interface of the network communication device.

38. A system for controlling access to a data store of user-specific information in a network computing environment being accessed by a client and a user, the system comprising:

a web-services system providing a software service to the user, said web-services system maintaining the data store of user-specific information in connection with the software service;

a data store of default access preferences, said default access preferences defining a list of predetermined access permissions allowed by the user with respect to the data store of user-specific information, the client desiring access to the data store of user-specific information and transmitting an access request message having a parameter indicative of a desired form of access to the data store of user-specific information;

an access control interface associated with the web-services system, said access control interface receiving the access request message and comparing the desired form of access to an access control list associated with the software service, said access control list identifying whether the user has granted the requested form of access requested by the client; and

an access control engine determining an intended use by the client of the user-specific information in the data store of user-specific information, said access control engine also determining a default access preference defining a list of default access

permissions to the data store of user-specific information that the user has allowed, the access control engine comparing the determined intended use and the default access permissions and dynamically creating an access control rule granting the desired access of the client if the intended use is permitted by the default access permissions.

39. The system of claim 38 wherein the access control interface comprises a service-side fabric associated with the software service provided by the web-services system.

40. A method of controlling access to user specific information by a third party in a network computing environment, said network computing environment including a web-services provider, a user of a service provided by the web-services provider, the web-services provider maintaining a data store of user-specific information associated with the user, the third party in digital communication with the web-services provider, the third party desiring access to the user-specific information in the data store, and the user communicating with the web-services provider via a network communication device having a display interface and a selection interface, said method of controlling access to user-specific information by the third party comprising:

obtaining at the web-services provider a digital request message from the third party desiring access to the user-specific information in the data store;

determining an intended purpose of the third party for accessing the user-specific information in the data store;

generating an option list having at least one entry therein based on the determined intended purpose of the third party for accessing the user-specific information in the data store;

displaying to the user on the display interface of the network communication device an option menu reflecting the generated option list, said option menu prompting the user to accept or reject at least one option using the selection interface of the network communication device;

receiving from the network communication device a selection signal indicative of whether the user accepted or rejected the at least one option; and

creating an access control rule based on the received selection signal, said access control rule defining an extent of access to the user-specific information in the data store granted to the third party.

41. One or more computer-readable media having computer-executable instructions for performing the method recited in claim 40.

42. A method of providing and selecting from a menu displayed on a display interface in a network computing environment, said network computing environment including a web-services provider, a user of a service provided by the web-services provider, the web-services provider maintaining a data store of user-specific information associated with the user, a third party in digital communication with the web-services provider, and the third party desiring access to the user-specific information in the data store, the user communicating with the web-services provider via a network communication device having the display interface and a user selection interface, said method comprising:

retrieving an intentions document associated with the third party desiring access to the user-specific information in the data store, said intentions document identifying:

a purpose for which the third party desires access to the user-specific information in the data store;

a value proposition associated with the purpose for which the third party desires access to the user-specific information in the data store; and

a method by which the third party proposes to access the user-specific information in the data store;

generating a set of menu entries, said menu entries identifying:

an identity of the third party;

the user-specific information in the data store to which the third party desires access;

the purpose for which the third party desires access to the user-specific information in the data store;

the value proposition associated with the purpose for which the third party desires access to the user-specific information in the data store;

the method by which the third party proposes to access the user-specific information in the data store;

displaying the menu entries on the menu on the display interface of the network communication device;

prompting the user to authorize or deny the third party to access the user-specific information in the data store; and

operatively receiving a selection signal being indicative of whether the user authorized or denied the third party to access the user-specific information in the data store, and creating an access control rule indicative of whether the user authorized the third party to access the user-specific information in the data store.

43. One or more computer-readable media having computer-executable instructions for performing the method recited in claim 42.

44. An access control engine for use in a network computing environment including a web-services provider providing a software service, a user of the software service provided by the web-services provider, and a client, said web-services provider maintaining a data store of user-specific information in connection with the software service, an access control list associated with the data store of user-specific information identifying existing access permissions to the data store of user-specific information, said web-services provider also maintaining a data store of user-specific default access preferences, and said client desiring access to the data store of user-specific information and transmitting an access request message to the web-services provider, the access control engine comprising:

schema for receiving and parsing the access request message, said schema identifying an intended use by the client of the user-specific information in the data store;

a validation engine, said validation engine determining if the existing access permissions identified in the access control list permit the client to access the data store of user-specific information for said identified intended use; and

a policy engine being invoked if the existing access permissions identified in the access control list do not permit the client to access the data store of user-specific information for the identified intended use, said policy engine dynamically determining an access control rule by comparing the user-specific default access preferences with said identified intended use, said validation engine writing said access control rule to the access control list.

45. The access control engine of claim 44 wherein the schema for receiving and parsing the access request message further identifies a method by which the client desires to access the user-specific information in the data store.

46. The access control engine of claim 45 wherein the validation engine determines if the existing access permissions identified in the access control list permit the client to access the data store of user-specific information using the identified method by which the client desires to access the user-specific information in the data store.